Bekannte Probleme mit Cisco XDR

Inhalt

[Einleitung](#)

[Bekannte Probleme:](#)

[Vorfälle](#)

[Untersuchungen](#)

[Cisco Integrationen](#)

[Integration mit Drittanbieterlösungen](#)

[Ressourcen](#)

[XDR Automatisieren](#)

[XDR-Analysen](#)

[Sicherer Client](#)

Einleitung

In diesem Artikel werden die derzeit bekannten technischen Probleme mit Cisco XDR beschrieben.

Technische Probleme können von Cisco anerkannt werden, werden derzeit geprüft, warten auf ihre Behebung oder gelten als normal.

Bekannte Probleme:

Vorfälle

1.- Die Option "Aufgabe nicht zutreffend markieren" wird nur bei der Erstellung von XDR-Vorfällen und nicht bei der Aktualisierung von Vorfällen berücksichtigt.

Status: Problem festgestellt und Lösung noch ausstehend

Details: Strategische Leitfäden zu Cisco XDR-Guided Response die Option zum Ausblenden Aufgaben, die nicht auf den aktuellen Incident zutreffen. Im Oktober 2024 hat Cisco eine Erweiterung von Cisco XDR veröffentlicht, mit der Aufgaben ohne entsprechende Observables automatisch ausgeblendet werden. Diese Verbesserung funktioniert, wenn ein Incident erstellt wird, bewertet aber die entsprechenden Aufgaben nicht, wenn sie aktualisiert werden.

Weitere Schritte: Cisco arbeitet an der Behebung dieses Problems.

Erwartete Auflösung: Dezember 2024

Untersuchungen

Derzeit sind keine Probleme mit dieser XDR-Funktion bekannt.

Cisco Integrationen

Derzeit sind keine Probleme mit dieser XDR-Funktion bekannt.

Integration mit Drittanbieterlösungen

1.- Microsoft-Kunden mit G-Typ-Lizenzen können die XDR-Microsoft-Integration nicht nutzen.

Status: Optimales Arbeiten

Details: Berechtigungen vom Typ Microsoft G werden nur für Regierungsbehörden in kontrollierten Umgebungen bereitgestellt.

Weitere Schritte: Cisco arbeitet mit Microsoft zusammen, um die Anforderungen zu verstehen, zu integrieren mit der Microsoft GCC-Umgebung, in der Ansprüche vom Typ Microsoft G werden bereitgestellt. Wenn durchführbar, Cisco XDR plant die Integration in Microsoft G-Lizenzen für Microsoft Defender for Endpoint, O365 und Entra.

Ressourcen

Derzeit sind keine Probleme mit dieser XDR-Funktion bekannt.

XDR Automatisieren

1.- XDR-Automatisierungsregeln für Vorfälle werden unerwartet nicht mehr ausgeführt

Status: Problem festgestellt und Lösung noch ausstehend

Details: Regeln für die Vorfallautomatisierung angetrieben durch Workflows und Trigger unerwartetes Beenden der Ausführung. Diese wird nicht angegeben in der XDR-Benutzeroberfläche, außer bei der Überprüfung die Kennzahlen für Workflows laufen über die Zeit. In diesem Fall werden die Workflows reduziert oder gar nicht ausgeführt, je nachdem, wie lange das Problem noch andauert.

Weitere Schritte: Cisco hat dieses Problem im XDR-Backend erkannt und arbeitet an seiner Lösung. Cisco plant außerdem die Implementierung zusätzlicher Überwachungs- und Statusüberwachungsfunktionen, um dieses Problem in Zukunft zu vermeiden.

Problemumgehung: Deaktivieren und Erneut aktivieren Sie die Regel, um einen Neustart der Auslösung und Verarbeitung der Workflowregel einzuleiten.

Erwartete Auflösung: Januar 2025

XDR-Analysen

Derzeit sind keine Probleme mit dieser XDR-Funktion bekannt.

Sicherer Client

1.- Die Bereitstellung sicherer Clients/Endpunkte wird durch Microsoft Intune/Microsoft Defender für Endgeräte-Updates beeinträchtigt, sodass eine ordnungsgemäße Installation verhindert wird.

Status: Optimales Arbeiten

Details: Fortlaufend: Dieses Problem betrifft Cisco XDR-Kunden, die Cisco Secure Client für Network Visibility Module (NVM) mit Cisco XDR installieren. Die Einstellungen von Microsoft Defender for Endpoint (über Intune konfiguriert) verhindern, dass Secure Client ordnungsgemäß installiert wird. Wenn eine Funktion in Microsoft Defender zur Reduzierung der Endpunktangriffsfläche in der Vorschau angezeigt wird, Reduzierung der Angriffsfläche - Blockverwendung kopierter oder imitierter Systemwerkzeuge (Vorschau) deaktiviert ist, kann die Installation erfolgen.

Weitere Schritte: Der Cisco Secure Client verhält sich bei der Installation wie erwartet. Microsoft Defender for Endpoint/Microsoft Intune verursacht jedoch unerwartete Störungen bei der Installation. Cisco hat eine Problemumgehung für Kunden gefunden, die von diesem Problem betroffen sind.

Problemumgehung: Es wird empfohlen, die Konfiguration für diese Funktion mit dem Anwendungsentwickler abzustimmen oder diese Funktion weiter zu verwenden. [Wissensdatenbank](#). Zur sofortigen Problembeseitigung können wir unseren verwalteten Endpunkt in Intune entweder in eine weniger restriktive Richtlinie ändern oder diese Funktion vorübergehend explizit deaktivieren, bis die entsprechenden Schritte unternommen werden. Diese Einstellung im Intune-Admin-Portal wurde als temporäre Maßnahme zur Wiederherstellung der sicheren Endpunkt-Konnektivität verwendet.

Weitere Informationen zu diesem Problem finden Sie hier. [Artikel](#).

Wenn Sie den Cisco Support kontaktieren müssen, folgen Sie den Anweisungen unter diesem [Link](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.